JOURNAL OF COMBINATORIAL THEORY, Series B 62, 44–62 (1994)

Existence and Explicit Constructions of $q+1$ Regular Ramanujan Graphs for Every Prime Power q

MOSHE MORGENSTERN*, †

Department of Mathematics, The Hebrew University, Jerusalem, Israel

Received February 21, 1992

For any prime power q, we give explicit constructions for many infinite linear families of $q+1$ regular Ramanujan graphs. This partially solves a problem that was raised by A. Lubotzky, R. Phillips, and P. Sarnak. They gave the same results as here, but only for q being prime and not equal to two, and raised the question of the existence and explicit construction of such graphs for other degrees of regularity. Moreover, our construction removes the nondeterministic part of finding large prime numbers, which for some applications may appear in their construction. Our graphs are given as Cayley graphs of PGL_2 or PSL_2 over finite fields, with respect to very simple generators. They also satisfy all other extremal combinatorial properties that those of Lubotsky, Phillips, and Sarnak do.

1. INTRODUCTION

An (n, r, d)-*expander* is a finite r regular undirected graph $\Gamma = (V, E)$, with $|V| = n$ ($|I| = |O| = n$ in case of a bipartite graph, $V = I \cup O$), such that for any set $S \subseteq V$ ($S \subseteq I$ when Γ is bipartite), the set of neighbors of S $\Gamma(S) = \{v \in V \mid (v, u) \in E \text{ for some } u \in S\}$ satisfies

$$|\Gamma(S)| \geq |S| + d(1 - |S|/n)\,|S|.$$

Over the last decade, expanding graphs have became one of the most useful tools in computational complexity. For example, expanding graphs play a crucial role in many lower bounds, asymptotically optimal algorithms, and designs of communication networks. (References for these and more, can be found in [Kl], for example). While it is generally easy to prove that expanders with various properties exist through probabilistic methods, explicit constructions have been much more difficult to obtain, although many applications require an explicit construction.

* E-mail: morgen@sunrise.huji.ac.il

† Part of this research was done while the author was at the department of Computer Science, The University of British Columbia, Vancouver, BC, Canada.

0095-8956/94 $6.00

Let Γ be a connected undirected r-regular graph with n vertices (n inputs and n outputs in case of a bipartite graph), and A its adjacency matrix. Clearly r is the largest eigenvalue of A and has multiplicity one. Denote the second largest eigenvalue by λ. It has been proved that:

THEOREM [Al, AM]. a. *Γ is an $(n, r, 1-\lambda^2/r^2)$-expander.*

b. *If Γ is an (n, r, d)-expander then $\lambda \leqslant r - d^2/8r$.*

c. *Let $\{\Gamma_i = (V_i, E_i)\}_{i=1}^{\infty}$ be an infinite family of r regular graphs. If $\lim_{i\to\infty} |V_i| = \infty$ then $\liminf_{i\to\infty} \lambda(\Gamma_i) \geqslant 2\sqrt{r-1}$.*

We see that every r regular graph is an expander for some d. But what we are looking for is a *linear family* of r regular expanders, i.e., a family $\{\Gamma_i = (V_i, E_i)\}_{i=1}^{\infty}$, s.t. every Γ_i is a $(|V_i|, r, d)$-expander, for fixed r and d, $|V_i| \to \infty$ linearly.

The first explicit construction for linear families of expanders was given by Margulis [Ma] and was improved by Gaber and Galil [GG]. It was known that much better families exist [Pin, Pip], but for a long time they were not found explicitly, until the Ramanujan graphs were built by Lubotzky, Phillips and Sarnak [LPS] (and independently by Margulis [Ma1] at the same time). The theorem above says that looking for a family of expanders with a good common d, is almost the same as looking for a family with a good common bound for λ, but for this the best we can expect is $\lambda \leqslant 2\sqrt{r-1}$.

DEFINITION 1.1. A *Ramanujan graph* is a connected finite r regular graph Γ; its second largest eigenvalue $\lambda(\Gamma)$ is smaller than or equal to $2\sqrt{r-1}$.

In [LPS], by use of representation theory of $PGL_2(Q_p)$ and Deligne's theorem (known as Ramanujan's conjecture), for every prime $p \neq 2$ a linear family of $p+1$ regular Ramanujan graphs is explicitly constructed. They raised the question of the existence and explicit construction of r regular Ramanujan graphs for other r's. Here we solve this partially, by working over function fields and by using Drinfeld's theorem [Dr] (instead of Deligne's). For every prime power q (including even q's) we explicitly construct many linear families of $q+1$ regular Ramanujan graphs.

Moreover, if in the [LPS] construction a family of graphs with increasing degrees of regularity is needed, or if one wants the graph to be a Cayley graph of $PGL_2(R)$ where R is a field, it requires that we find an increasing sequence of prime numbers, which is not of polynomial time by a deterministic machine. In our construction, we may keep the characteristic of the finite fields fixed (and small); then only a sequence of irreducible

polynomials (of increasing degrees) over this small prime field is needed. This can be done in polynomial time, by the algorithm of Shoup [Sh].

Our graphs are gives as Cayley graphs of PGL_2 or PSL_2 over finite fields, with respect to very simple generators and also have all other combinatorial properties that those of [LPS] do. Our main results are summarized in Theorems 4.13 and 5.13.

In Section 2 we present the background about the discrete valuations of $\mathbb{F}_q(x)$, the local tree of PGL_2, and quaternion algebras over $\mathbb{F}_q(x)$. In Section 3 the abstract construction is given, and we prove that the results are Ramanujan graphs. Then in Sections 4–5 we derive explicit constructions from this abstract one. Section 4 deals with odd prime powers q, and Section 5 with even q's. Sections 4–5 can be read without reading Section 3.

2. Background

Let q be a prime power, and $\mathbb{F}_q$ the field with q elements, $\mathbb{F}_q[x]$ the polynomials over $\mathbb{F}_q$ and $k=\mathbb{F}_q(x)$ its quotient field. For every irreducible $f\in\mathbb{F}_q[x]$, the *discrete valuation* v_f on k is defined by $v_f(g/h)=\mathrm{ord}_f(g)-\mathrm{ord}_f(h)$, where $\mathrm{ord}_f(g)$ is the maximal power n s.t. f^n divides g. The valuation at $1/x$ (also called the valuation at infinity) is defined by $v_{1/x}(g/h)=\mathrm{degree}(h)-\mathrm{degree}(g)$. These are all discrete valuations of k; they are called the *places* of k. For a place p let k_p be the completion of k with respect to the metric $|a|=q^{-v_p(a)}$, and O_p its integers. $k_p=\mathbb{F}_q((p))$ is the field of Laurent series in p over $\mathbb{F}_q$, and $O_p=\mathbb{F}_q[[p]]$ is the ring of Taylor series in p over $\mathbb{F}_q$.

For an algebraic group $\mathbf{H}$ defined over k, we will always denote by H_* its point over $*$, e.g., H_k, H_{k_p}, H_{O_p} (the only exception for these notations is H_p which means H_{k_p}). Our notations will be

$$\mathbf{G}'=PGL_2,\qquad \mathbf{G}=\{\xi\in\mathscr{A}\mid N(\xi)\neq 0\}/Z,\qquad \mathbf{G}^1=\{\xi\in\mathscr{A}\mid N(\xi)=1\}/Z, \tag{1}$$

where PGL_2 is the group of 2×2 invertible matrices divided by its center, $\mathscr{A}$ is a fixed quaternion algebra, and "$/Z$" means "divided by its center."

The *Adele group* of H is defined by

$$H_{\mathbb{A}}=\left\{(\ldots,g_p,\ldots)\in\prod_p H_p \;\middle|\; g_p\in H_{O_p}\text{ almost everywhere}\right\}$$

where by "almost everywhere" we mean: except for a finite number of places. Multiplication is componentwise. A topology on $H_{\mathbb{A}}$ is defined by declaring the subgroup $\prod_p H_{O_p}$ with the usual Tychonof product topology to be open. With this topology, $H_{\mathbb{A}}$ is a locally compact group H_k is

embedded naturally into $H_{\mathbb{A}}$ by $g \to (g, g, ..., g, ...)$ (see [GGPS], e.g., for more details).

In [Se, Section II.1] the structure of the $q^{\text{degree}(p)}+1$ regular tree is put on G'_p/G'_{O_p} (where degree$(1/x)=1$). The tree $T_p = G'_p/G'_{O_p}$ is completely described by saying that the neighbors of gG'_{O_p} are the $q^{\deg(p)}+1$ matrices $gs_iG'_{O_p}$, $i=1, ..., q^{\deg(p)}+1$, where

$$\{s_1, ..., s_{q^{\deg(p)}+1}\} = \left\{ \begin{pmatrix} p & b \\ 0 & 1 \end{pmatrix} \middle| \begin{array}{c} b \in \mathbb{F}_q[x] \\ \deg(b) < \deg(p) \end{array} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \right\}. \tag{2}$$

From this point of view it is clear that G'_p acts on T_p (from the left) as a group of automorphisms.

A *quaternion algebra* over $k = \mathbb{F}_q(x)$ is a skewfield $\mathscr{A}$ with center k, that has degree 4 as a vector space over k. It is well knwon (a proof can be found in [Alb, Theorem 26]) that there is a basis of the form **1**, **i**, **j**, **ij**, for $\mathscr{A}$ over k. The minimal polynomial of **i** over k has degree 2, and let $\bar{\mathbf{i}}$ be its algebraic conjugate, the same is true for **j** and **ij**. For a quaternion $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij}$, this defines its *conjugate* $\bar{\xi} = a + b\bar{\mathbf{i}} + c\bar{\mathbf{j}} + d\bar{\mathbf{ij}}$, the *trace* $\text{tr}(\xi) = \xi + \bar{\xi}$, and the *norm* $N(\xi) = \xi\bar{\xi}$. By definition $\text{tr}(\xi)$, $N(\xi) \in k$, and ξ is invertible iff $N(\xi) \neq 0$. Since $(\mathbf{ij})^2 - (\mathbf{ij} + \bar{\mathbf{ij}})\,\mathbf{ij} + \mathbf{ij}\bar{\mathbf{ij}} = 0$, we see that $\overline{\mathbf{ij}} = \bar{\mathbf{ij}}$. Hence $\overline{\xi_1\xi_2} = \overline{\xi_2}\,\overline{\xi_1}$ and $N(\xi_1\xi_2) = N(\xi_1)\,N(\xi_2)$.

An *order* in $\mathscr{A}$, is a subring of $\mathscr{A}$ which is finitely generated as an $\mathbb{F}_q[x]$ submodule, and contains a basis for $\mathscr{A}$ (over k), its first element being **1**. A *maximal order* is an order which is not included in any other order. An *integral set* is a maximal order which contains **i**, **j**, **ij**. Let $\mathscr{S}$ be an integral set, ξ is a *unit* in $\mathscr{S}$ if $\xi^{-1} \in \mathscr{S}$. We say that $\mathscr{A}$ has *class number* 1 if $\mathscr{S}$ (and hence very other maximal order) is a principle ideal ring.

The following is a key theorem for the explicit constructions.

THEOREM 2.1 [To, Theorem 10]. *Let $\mathscr{A}$ have class number* 1, *$\mathscr{S}$ be an integral set, and $\xi \in \mathscr{S}$ be indivisible by a polynomial in $\mathbb{F}_q[x]$. If $N(\xi) = f_1 \cdots f_n$ where the f_i are irreducible in $\mathbb{F}_q[x]$, then $\xi = \pi_1 \cdots \pi_n$ where $N(\pi_i) = f_i$. π_1 is unique except for multiplication by a unit of $\mathscr{S}$ on the right, $\pi_2, ..., \pi_{n-1}$ are unique but for multiplication by units on the right or left, and π_n is unique except for left unit factors.*

Proof. By induction on n. Let η be the generator of the (left) ideal created by ξ and f_n. So $\xi = \mu\eta$ and η is unique except for multiplication by a unit on the left (this gives the unit which multiplies μ from the right). Since $\eta \mid f_n$ and we know that $\eta \neq f_n$ (since f_n does not divide ξ), $N(\eta) \mid N(f_n) = f_n^2$ but $N(\eta) \neq f_n^2$, so $N(\eta) = f_n$ and we can continue with μ. ∎

We say that $\mathcal{A}$ is *ramified* at a place p, if $\mathcal{A}_p$ is still a skewfield. By well-known structure theorems of central simple algebras (see [Di, Alb, Re], e.g.), the only other possibility is that $\mathcal{A}_p \cong M_2(k_p)$, then we say that $\mathcal{A}$ *splits* at p. In this case, for any maximal order M of $\mathcal{A}$, it is possible to have $\theta: \mathcal{A}_p \cong M_2(k_p)$ s.t.

$$\operatorname{tr}(\xi) = \operatorname{tr}(\theta(\xi)), \qquad N(\xi) = \det(\theta(\xi)), \qquad \theta(M) = M_2(O_p). \tag{3}$$

By theorems of Eichler and Hasse ([Re, Theorems 32.11, 32.13], e.g.) there are only a finite number of places in which $\mathcal{A}$ is ramified; this number is even and not zero.

One of the basic toolds we use to prove the abstract construction, but also to recover things about the explicit construction, is the *strong approximation Theorem*. Let $\mathbf{H} = SL_2$, $\mathbf{H} = \mathbf{G}^1$, or $\mathbf{H} = k$.

THEOREM 2.2 [Pr; Vi, Theorem 4.3]. *Let S be a set of places of k such that $\prod_{p \in S} H_p$ is not compact, then $H_k \prod_{p \in S} H_p$ is dense in $H_{\mathbb{A}}$.*

3. ABSTRACT CONSTRUCTION

Let $\mathcal{A} = k\mathbf{1} + k\mathbf{i} + k\mathbf{j} + k\mathbf{ij}$ be a quaternion algebra over $k = \mathbb{F}_q(x)$, which is ramified at $1/x$, and p is a finite place (i.e., $p \neq 1/x$) in which $\mathcal{A}$ splits. Let $\mathcal{R} = \mathbb{F}_q[x, 1/p]$ be the minimal subring of k which contains $\mathbb{F}_q$, x, and $1/p$, and $\Gamma(1) = G_{\mathcal{R}}$ (see (1) for the notations). (Since an element $\xi \in \mathcal{A}_{\mathcal{R}}$ is invertible in $\mathcal{A}_{\mathcal{R}}$ iff $N(\xi)$ is so in $\mathcal{R}$, the group $\mathcal{A}^*_{\mathcal{R}}$ of all invertible elements in $\mathcal{A}_{\mathcal{R}}$ is

$$\mathcal{A}^*_{\mathcal{R}} = \{\xi \in \mathcal{A}_{\mathcal{R}} \mid N(\xi) = ap^n, a \in \mathbb{F}_q^*, n \in Z\},$$

so

$$\Gamma(1) = \mathcal{A}^*_{\mathcal{R}}/Z(\mathcal{A}^*_{\mathcal{R}}) = \mathcal{A}^*_{\mathcal{R}}/\{ap^n \mid a \in \mathbb{F}_q, n \in Z\}. \tag{4}$$

Understanding this makes clear how the explicit constructions that we will give later result from this abstract construction).

Let $g(x) \in \mathbb{F}_q[x]$ be any polynomial prime to p and to any other finite place in which $\mathcal{A}$ is ramified. Since after multiplying by a suitable power of p, every $\xi \in \Gamma(1)$ can be represented by a quaternion with coefficients in $\mathbb{F}_q[x]$ and $(p, g) = 1$, we may define

$$\Gamma(g) = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \Gamma(1) \mid b \equiv c \equiv c \equiv 0 \bmod g(x), (a, g) = 1\}. \tag{5}$$

$\Gamma(g) \subseteq G_p \cong PGL_2(k_p) = G'_p$ (since $\mathcal{A}$ splits at p).

LEMMA 3.1. *$\Gamma(g)$ is a co-compact lattice in G_p (i.e., $\Gamma(g)$ is discrete in G_p and $\Gamma(g)\backslash G_p$ is compact).*

Proof. Since $|\Gamma(1):\Gamma(g)|<\infty$ it is enough to prove it for $\Gamma(1)$. Let $K^1=\prod_{f\neq p,\,1/x} G^1_{O_f}$; clearly $G^1_{1/x}G^1_pK^1$ is a nonempty open subset of $G^1_{\mathbb{A}}$. Since $\mathscr{A}$ is ramified at $1/x$ and splits at p, $G^1_{1/x}$ is compact but $G^1_p\cong SL_2(k_p)$ and hence $G^1_{1/x}G^1_p$ are not. By Theorem 2.2 $G^1_kG^1_{1/x}G^1_p$ is dense in $G^1_{\mathbb{A}}$, so

$$G^1_{\mathbb{A}}=G^1_kG^1_{1/x}G^1_pK^1. \tag{6}$$

But $G^1_k\cap K^1=G^1_{\mathscr{A}}$; therefore,

$$G^1_{\mathscr{A}}\backslash G^1_{1/x}G^1_p\cong G^1_k\backslash G^1_{\mathbb{A}}/K^1. \tag{7}$$

By [We, Chap. IV, Theorems 2.2, 3.4] $G^1_k\backslash G^1_{\mathbb{A}}$ is compact, and from (7) so is $G^1_{\mathscr{A}}\backslash G^1_p$. But $|G_p:G^1_p|<\infty$ (since $|O_p^*:O_p^{*2}|<\infty$), so $G^1_{\mathscr{A}}\backslash G_p$ and hence $G_{\mathscr{A}}\backslash G_p=\Gamma(1)\backslash G_p$ are compact.

Assume that $\{\gamma_n\}\subseteq\Gamma(1)$ is a sequence which proves that $\Gamma(1)$ is not discrete in G_p. Since $\mathscr{A}$ is ramified at $1/x$, so that $G_{1/x}$ is compact, we may assume that $\{\gamma_n\}\subseteq G_{1/x}$ converges. Hence, $\{\gamma_n\}\subsetneq G_{1/x}G_p$ diagonally proves that the diagonal embedding of $\Gamma(1)$ into $G_{1/x}G_p$ is not discrete. This obviously is not true, since the valuations at $1/x$ and p are opposite to one another. ∎

Look at the action of $\Gamma(g)$ (from the left) on the $q^{\deg(p)}+1$ regular tree $T_p=G'_p/G'_{O_p}=G_p/G_{O_p}$. Since T_p is discrete, the quotient $\Gamma(g)\backslash G_p/G_{O_p}$ of T_p by the discrete subgroup $\Gamma(1)$, is discrete. By Lemma 3.1 it is also compact; i.e., it is a finite graph.

THEOREM 3.2. *If $\mu\neq\pm(q^{\deg(p)}+1)$ is an eigenvalue of the adjacency matrix of $\Gamma(g)\backslash G_p/G_{O_p}$, then $|\mu|\leqslant 2\sqrt{q^{\deg(p)}}$. In particular $\Gamma(g)\backslash G_p/G_{O_p}$ is a Ramanujan graph.*

Proof. We are not going to give much detail, since the proof is almost the same as that which is given in [Lu] for the global field Q. A detailed proof for our case when the global field is $F_q(x)$, can be found in [Mo].

Let ρ be a continuous irreducible unitary representation of G'_p in $(H,\langle\ ,\ \rangle)$. Assume that ρ is of class one; i.e., there is a $v\in H$ s.t. $\|v\|=1$ and $G'_{O_p}\cdot v=v$. $f_\rho(g)=\langle gv,v\rangle$ is called the spherical function of ρ ($f_\rho: G'_p\to C$). Since at most one such v can exist, f_ρ is well defined.

Let $U=G'_{O_p}\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)G'_{O_p}$, 1_U its characteristic function, and define the convolution $(f*h)(x)=\int_{G'_p}f(xy^{-1})\,h(y)\,dy$. There is a $\mu\in C$ s.t. $f_\rho*1_U=\mu f_\rho$, and then ρ is denoted by ρ^μ. For more details see [La, Chap. IV].

LEMMA. *μ is an eigenvalue of the adjacency matrix A of $\Gamma(g)\backslash G'_p/G'_{O_p}$ iff the representation ρ^μ appears in the (right) regular representation $R_{G'_p}$*

of G'_p in $L_2(\Gamma(g)\backslash G'_p)$. Moreover, if $\mu \neq \pm(q^{\deg(p)}+1)$ then ρ^μ is not one-dimensional.

Proof. Assume that there is an $e \in L_2(\Gamma(g)\backslash G'_p/G'_{O_p})$ s.t. $\|e\|=1$ and $Ae=\mu e$, in particular, $e \in L_2(\Gamma(g)\backslash G'_p)$ and $R_{G'_p}(G'_{O_p})\cdot e = e$. Let ρ be the irreducible subrepresentation (submodule) of $R_{G'_p}$ which contains e; clearly $f_\rho(g)=\langle ge, e\rangle$. A simple calculation shows that $f_\rho * 1_U = \mu f_\rho$, so $\rho=\rho^\mu$ appears in $L_2(\Gamma(g)\backslash G'_p)$.

Assume that ρ^μ appears in $L_2(\Gamma(g)\backslash G'_p)$, and let f be its G'_{O_p} fixed vector, so that $f \in L_2(\Gamma(g)\backslash G'_p/G'_{O_p})$. A simple calculation shows that $Af=\mu f$ and that μ is an eigenvalue of A.

Assume that ρ^μ is one-dimensional; then $H=\langle f\rangle$ with $G'_{O_p}\cdot f = f$ and ρ^μ is trivial on G'_{O_p}. It must also be trivial on $PSL_2(k_p)$ which is simple. But $|G'_p : PSL_2(k_p)\, G'_{O_p}| = 2$, so the only possibilities for the spherical function are trivial; i.e., $\rho^\mu = 1$ and $\mu = q^{\deg(p)}+1$, or give the values $\{\pm 1\}$ which is easily seen to be the spherical function of $\rho^{-(q^{\deg(p)}+1)}$. ∎

Let $g(x)=\prod_{i=1}^{l} g_i(x)^{n_i}$, where $g_i \in \mathbb{F}_q[x]$ are irreducible and $g_i \neq g_j$ for $i \neq j$. Let

$$K_r = \begin{cases} \operatorname{Ker}\{G_{O_r} \xrightarrow{\alpha} G(O_r/r^{n_i}O_r)\}, & r=g_i,\ 1\leqslant i\leqslant l, \\ K_r = G_{O_r}, & r \neq g_i, \end{cases}$$

where

$$\alpha(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij}) = (a \bmod r^{n_i}) + (b \bmod r^{n_i})\,\mathbf{i} + (c \bmod r^{n_i})\,\mathbf{j} + (d \bmod r^{n_i})\,\mathbf{ij}.$$

Let $K=\prod_{f\neq p,\,1/x} K_f$ and $H = G_k G_{1/x} G_p K$. Since $|\prod_{f\neq p,\,1/x} G_{O_f} : K| < \infty$ and, by (6), $G^1_{\mathbb{A}} = G^1_k G^1_{1/x} G^1_p K^1$, and, since by Theorem 2.2, $k^*_{\mathbb{A}} = k^* k^*_{1/x} k^*_p \prod_f O^*_f$, it is clear that H contains a finite index subgroup of $G^1_{\mathbb{A}} k^*_{\mathbb{A}}$. It is well known that $|G_{\mathbb{A}} : G^1_{\mathbb{A}} k^*_{\mathbb{A}}| < \infty$, and hence $|G_{\mathbb{A}} : H| < \infty$, and also $|G_k\backslash G_{\mathbb{A}}/K : G_k\backslash H/K| < \infty$. Since $G_k \cap K = \Gamma(g)$,

$$G_k\backslash H/K \cong \Gamma(g)\backslash G_{1/x} G_p$$

as $G_{1/x}G_p$ modules (by multiplication from the rigth), and

$$|G_k\backslash G_{\mathbb{A}}/K : \Gamma(g)\backslash G_{1/x}G_p| < \infty.$$

Therefore, for every irreducible representation $\tau_{1/x}\otimes\tau_p$ of the (right) regular representation of $G_{1/x}G_p$ in $L_2(\Gamma(g)\backslash G_{1/x}G_p)$, there is an irreducible subrepresentation $\delta = \bigotimes_f \delta_f$ of the regular representation of $G_{\mathbb{A}}$ in $L_2(G_k\backslash G_{\mathbb{A}})$, s.t. $\delta_{1/x}=\tau_{1/x}$ and $\delta_p = \tau_p$.

Assume now that $\mu \neq \pm(q^{\deg(p)+1})$ is an eigenvalue of the adjacency matrix of $\Gamma(g)\backslash G_p/G_{O_p} = \Gamma(g)\backslash G'_p/G'_{O_p}$. By the lemma, ρ^μ (which is not one-dimensional) appears in the regular representation of G_p in $L_2(\Gamma(g)\backslash G_p)$, so $\rho = 1 \otimes \rho^\mu$ appears in $L_2(\Gamma(g)\backslash G_{1/x}G_p)$, and, hence, $\delta = \otimes_f \delta_f$ with $\delta_p = \rho^\mu$ appears in the regular representation of $G_{\mathbb{A}}$ in $L_2(G_k\backslash G_{\mathbb{A}})$. By the Jacquet Langlands correspondence [Ge, Th. 10.5] there is a cuspidal subrepresentation $\chi = \otimes_f \chi_f$ of $G'_{\mathbb{A}}$ in $L_2(G'_k\backslash G'_{\mathbb{A}})$ s.t. $\chi_p = \delta_p = \rho^\mu$. By the theorem of Drinfeld [Dr], $\rho^\mu = \chi_p$ is a principle series representation, i.e., $|\mu| \leqslant 2\sqrt{q}$. ∎

4. Explicit Construction for Odd q's

Let us choose the quaternion algebra

$$\mathscr{A} = k\mathbf{1} + k\mathbf{i} + k\mathbf{j} + k\mathbf{ij}, \qquad \mathbf{i}^2 = \varepsilon, \quad \mathbf{j}^2 = x - 1, \quad \mathbf{ij} = -\mathbf{ji},$$

where ε is not a square in $\mathbb{F}_q$, and $k = \mathbb{F}_q(x)$. Here, $\bar{\mathbf{i}} = -\mathbf{i}$, $\bar{\mathbf{j}} = -\mathbf{j}$, $\bar{\mathbf{ij}} = -\mathbf{ij}$ so for $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij}$, $\bar{\xi} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{ij}$, $\operatorname{tr}(\xi) = 2a$, and

$$N(\xi) = a^2 - b^2\varepsilon + (d^2\varepsilon - c^2)(x-1). \tag{8}$$

If $N(\xi) = 0$, it happens also for a ξ with coefficients in $\mathbb{F}_q[x]$, which is impossible for $\xi \neq 0$ by Lemma 4.2, so $\mathscr{A}$ is a skewfield. Computing the discriminant of $\mathscr{A}$ we see that the only finite place in which $\mathscr{A}$ is ramified is $x-1$, so in order to have an even number of such places, $1/x$ must also be ramified. By [To, Theorem 1]

$$\mathscr{S} = \mathbb{F}_q[x]\,\mathbf{1} + \mathbb{F}_q[x]\,\mathbf{i} + \mathbb{F}_q[x]\,\mathbf{j} + \mathbb{F}_q[x]\,\mathbf{ij}$$

is an integral set in $\mathscr{A}$.

Lemma 4.1 [To]. *The class number of $\mathscr{A}$ is one.*

Proof. We will show that there is an Euclidean norm in $\mathscr{S}$. Let $\xi = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{ij} \in \mathscr{S}$, let $0 \neq m \in \mathbb{F}_q[x]$, and let $a_e = q_e m + r_e$ with $\operatorname{degree}(r_e) < \operatorname{degree}(m)$ for $e = 1, 2, 3, 4$, then $r = r_1 + r_2\mathbf{i} + r_3\mathbf{j} + r_4\mathbf{ij} \in \mathscr{S}$ and $\operatorname{degree}(N(r)) < \operatorname{degree}(N(m))$. Let now $\theta \in \mathscr{S}$ be another quaternion and $N(\theta) = m$, as we have shown we can divide $\xi\bar{\theta}$ by m and find $q, r \in \mathscr{S}$ such that $r = \xi\bar{\theta} - qm = \xi\bar{\theta} - q\theta\bar{\theta} = (\xi - q\theta)\,\bar{\theta}$ and degree $(N(r)) <$ $\operatorname{degree}(N(m)) = 2\operatorname{degree}(N(\theta))$. So $\operatorname{degree}(N(\xi - q\theta)) < \operatorname{degree}(N(\theta))$ and $\operatorname{degree}(N(\cdot))$ is the desired Eucliden norm. ∎

Let

$$N_z = \{\xi \in \mathscr{S} \mid N(\xi) = z\}.$$

LEMMA 4.2. a. $N_0 = \{0\}$, $|N_1| = q+1$.

b. $|N_x| = (q+1)^2$.

c. *Let N_1 act (by multiplication) from the left on N_x. In every one of the $q+1$ cosets of $N_1\backslash N_x$ there is a unique representative $1+\gamma\mathbf{j}+\delta\mathbf{ij}$, where $\gamma, \delta \in \mathbb{F}_q$ is one of the $q+1$ solutions in $\mathbb{F}_q$ for $\delta^2\varepsilon - \gamma^2 = 1$.*

Proof. a. Assume that $\xi = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij} \in N_0 \cup N_1$. Let γ, δ be the leading coefficients of c, d, and $d_1 = \max\{\deg(a), \deg(b)\}$, $d_2 = \max\{\deg(c), \deg(d)\}$. If $d_2 \geq d_1$, then in order to have in (8) $\deg(N(\xi)) \leq 0$, $\delta^2\varepsilon - \gamma^2$ must be zero which is impossible, so $d_1 > d_2$. Since $\alpha^2 - \beta^2\varepsilon \neq 0$, we have

$$0 \geq \deg(N(\xi)) = \deg(a^2 - b^2\varepsilon) > \deg((d^2\varepsilon - c^2)(x-1))$$

and we conclude that $d = c = 0$ and $a, b \in \mathbb{F}_q$. Clearly $\xi \in N_0$ is impossible for $\xi \neq 0$, since then $a^2 - b^2\varepsilon = 0$, but $\xi \in N_1$ can happen when $a^2 - b^2\varepsilon = 1$. As we will see right away, this last equation has exactly $q+1$ solutions, so $|N_1| = q+1$.

For u, v, $w \in \mathbb{F}_q$, the number of solutions of $uX^2 + vY_2 = w$ with $X, Y \in \mathbb{F}_q$, is $q-\eta$ if $w \neq 0$ and $q(\eta+1)$ for $w = 0$, where $\eta = 1$ if $-uv$ is a square in $\mathbb{F}_q$, and $\eta = -1$ if it is not. See, e.g., [Co, Corollary 1 to Theorem 10].

b. Assume that $N(\xi) = x$. If $d_1 > d_2$, since $\deg(a^2 - b^2\varepsilon)$ is even, in order to have $N(\xi) = x$ in (8) $\alpha^2 - \beta^2\varepsilon$ must be zero, which cannot happen, so $d_2 \geq d_1$. But since $\delta^2\varepsilon - \gamma^2 \neq 0$, $d, c \in \mathbb{F}_q$, and $d^2\varepsilon - c^2 = 1$, which causes $a, b \in \mathbb{F}_q$ and $a^2 - b^2\varepsilon = 1$. This again gives $(q+1)^2$ solutions.

c. The $q+1$ quaternions of $\mathscr{S}$,

$$\xi_i = 1 + \gamma_i\mathbf{j} + \delta_i\mathbf{ij} \qquad \text{s.t.} \quad \delta_i^2\varepsilon - \gamma_i^2 = 1, \quad i = 1, \ldots, q+1, \tag{9}$$

are as needed. Because $u \in N_1$ is of the form $u = \eta + \mu\mathbf{i}$ (see the proof of part a), we have $u\xi_i = \eta + \mu\mathbf{i} + \cdots$. So if $u\xi_i$ is also one of the $q+1$ quaternions of (9), we obtain $\eta = 1$, $\mu = 0$, and $u\xi = \xi$. This shows that no two quaternions of (9) appear in the same class of $N_1\backslash N_x$. But $|N_1\backslash N_x| = q+1$, so every class has exactly one representative. ∎

DEFINITION 4.3. $\xi_1, \ldots, \xi_{q+1}$ of (9) are called the *basic norm* x. Since ξ is a basic norm x iff $\bar{\xi}$ is so, we can assume that $\xi_1, \ldots, \xi_{\frac{q+1}{2}}$ are inconjugate to one another, and $\xi_i = \xi_{\frac{q+1}{2}+i}$.

LEMMA 4.4. *A quaternion $t \in \mathscr{S}$ with $N(t) = x^n$ for some integer n has the unique factorization*

$$t = x^r u\theta_1 \cdots \theta_m, \tag{10}$$

where $2r+m=n$, $N(u)=1$, θ_i *are basic norm* x, *and* x *does not divide* $\theta_1 \cdots \theta_m$.

Proof. Let x^r be the maximal power of x dividing t. By Theorem 2.1 and Lemma 4.1 we obtain a unique factorization (up to units) $t/x^r = \pi_1 \cdots \pi_m$ with $N(\pi_i) = x$. For a unique unit v of $\mathscr{S}$ $v\pi_m = \theta_m$ is a basic norm x and, of course, $N(v) = N(\theta_m)/N(\pi_m) = 1$. Looking at $\pi_1 \cdots \pi_m = \pi_1 \cdots \pi_{m-1} v^{-1} \theta_m$ and doing the same for $\pi_{m-1} v^{-1}$ etc., we finally obtain $t/x^r = u\theta_1 \cdots \theta_m$ uniquely. ∎

THEOREM 4.5. *A quaternion* $t = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \mathscr{S}$ *with* $N(t) = x^n$ *for some integer* n *is a multiple of basic norm* x *iff*

$$a - 1, b \equiv 0 \bmod(x-1). \tag{11}$$

Proof. A basic norm x satisfies (11), and it is easily seen that (11) is preserved under multiplication of quaternions. On the other hand, ξ has the factorization (10), in which $x^r\theta_1 \cdots \theta_m$ is a multiple of basic norm x ($x \in \xi\bar{\xi}$), and hence satisfies (11). In this factorization of t, u must be one, since after multiplying $x^r\theta_1 \cdots \theta_m$ by any other u, (11) will not hold. ∎

DEFINITION 4.6.

$$\Lambda(x-1) = \left\{ t = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \mathscr{S} \;\middle|\; \begin{array}{l} a - 1, b \equiv 0 \bmod(x-1), \\ N(t) \text{ is a power of } x, \\ x \text{ does not divide } t. \end{array} \right\}$$

COROLLARY 4.7. $\Lambda(x-1)$ *is a free group, and* $\xi_1, \ldots, \xi_{\frac{q+1}{2}}$ *of Definition* 4.3 *are free generators.*

Proof. Follows immediately from Lemma 4.4 and Theorem 4.5. ∎

Since our algebra $\mathscr{A}$ splits at x, there is an isomorphism

$$\theta: \mathscr{A}_x \cong M_2(k_x)$$

which satisfies (3), and clearly $\theta: \Lambda(x-1) \subsetneq PGL_2(k_x) = G'_x$. We shall identify $\Lambda(x-1)$ and its image in G'_x. Let $\Lambda(x-1)$ act by multiplication form the left on the $q+1$ regular tree $T_x = G'_x/G'_{O_x}$.

LEMMA 4.8. *The action of* $\Lambda(x-1)$ *on* T_x *is simply transitive (i.e., transitive and without stabilizers). Moreover,* T_x *can be viewed as the Cayley graph of* $\Lambda(x-1)$ *w.r.t. the basic norm* x *as generators.*

Proof. Since $\Lambda(x-1) \subseteq \Gamma(1)$ of (4) (for $p=x$), it is discrete in G_x by Lemma 3.1. A subgroup of G_x which stabilizes a vertex is compact, [Se, Excercises to Chap. II, Section 1.1]. So if $\gamma \in \Lambda(x-1)$ stabilizes a vertex, then $\{\gamma^n \mid n \in Z\}$ is discrete and compact and, hence, finite. This is impossible since $\Lambda(x-1)$ is a free group.

From the description of T_x in (2) we see that the distance of gG'_{O_x} from $1G'_{O_x}$ (the root of the tree) is $v_x(\det(g))$. So the basic norm x takes $1G'_{O_x}$ to its immediate neighbors, and if $\xi_1 G'_{O_x} = \xi_2 G'_{O_x}$, then $\xi_2^{-1}\xi_1$ stabilizes $1G'_{O_x}$ which is impossible for $\xi_1 \neq \xi_2$. Therefore, the $q+1$ neighbors of $1G'_{O_x}$ are given exactly by the $q+1$ basic norm x. Continuing this, we see that $\xi_i \xi_j G'_{O_x}$, $j=1, ..., q+1$, are all the $q+1$ neighbors of $\xi_i G'_{O_x}$, etc. Hence, every vertex of T_x is reachable with element of $\Lambda(x-1)$. ∎

Let $g(x) \in \mathbb{F}_q[x]$ be prime to $x(x-1)$ and $d = \text{degree}(g(x))$.

DEFINITION 4.9. $\Lambda(g) = \{\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \Lambda(x-1) \mid b, c, d \equiv 0 \bmod g(x),\ (a, g) = 1\}$. $\Gamma_g = \Lambda(g)\backslash T_x$ $(= \Lambda(g)\backslash G'_x / G'_{O_x} = \Lambda(g)\backslash\Lambda(x-1))$.

THEOREM 4.10. *Γ_g is a finite $q+1$ regular graph. Moreover, Γ_g is the Cayley graph of the group $\Lambda(g)\backslash\Lambda(x-1)$ w.r.t. the $q+1$ basic norm x as generators.*

Proof. Since $\Lambda(g(x)) \supseteq \Gamma((x-1)\, g(x))$ (see (5)), and by Lemma 4.8 T_x is identified with $\Lambda(x-1)$; our graph $\Gamma_g = \Lambda(g)\backslash\Lambda(x-1)$ is covered by

$$\widehat{\Gamma_g} = \Gamma((x-1)\, g(x))\backslash G'_x / G'_{O_x}. \tag{12}$$

$\widehat{\Gamma_g}$ is finite, since by Lemma 3.1 it is compact and discrete, so Γ_g is also finite. By Lemma 4.8 T_x is the Cayley graph of $\Lambda(x-1)$ w.r.t. the basic norm x as generators, but no two basic norm x are equivalent modulo $\Lambda(g)$, so the quotient $\Lambda(g)\backslash\Lambda(x-1)$ is a claimed. ∎

THEOREM 4.11. *Let μ be any eigenvalue of the adjacency matrix of Γ_g; if $u \neq \pm(q+1)$, then $|\mu| \leqslant 2\sqrt{q}$. In particular, Γ_g is a Ramanujan graph.*

Proof. As in (12), Γ_g is covered by $\widehat{\Gamma_g}$ which by Theorem 3.2 is as needed. Every function $f \in L_2(\Gamma_g)$ can be lifted to a function $\hat{f} \in L_2(\widehat{\Gamma_g})$ s.t. as operators, the adjacency matrices A and $\hat{A}$ give the same results. If $\hat{v}$ lies above v, then by definition $\hat{f}(\hat{v}) = f(v)$, and we have $\hat{A}(\hat{f})(\hat{v}) = A(f)(v)$. (Recall that as an operator $A(f)(v) = \sum_{u \text{ a neighbor of } v} f(u)$). So every eigenvalue of Γ_g is also an eigenvalue of $\widehat{\Gamma_g}$, and hence Γ_g is, as needed. ∎

For the sake of simplicity, let us assume from now on that $g(x)$ is irreducible of even degree d. (Since $\mathscr{A}$ splits at every factor of $g(x)$, similar

results can be achieved with much weaker assumptions on $g(x)$). By our assumption there is an $\mathbf{i} \in \mathbb{F}_{q^d}$ s.t. $\mathbf{i}^2 = \varepsilon$. Define $\mu: \Lambda(x-1) \to PGL_2(\mathbb{F}_{q^d})$

$$\mu(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij}) = \begin{pmatrix} a-b\mathbf{i} & c-d\mathbf{i} \\ (x-1)(c+d\mathbf{i}) & a+b\mathbf{i} \end{pmatrix}. \tag{13}$$

The kernel of μ is Λ_g, so the range of μ which is isomorphic to Γ_g is the Cayley graph of $\mu(\Lambda(x-1))$ with respect to the $q+1$ generators:

$$\mu(\xi_k) = \begin{pmatrix} 1 & \gamma_k - \delta_k \mathbf{i} \\ (\gamma_k + \delta_k \mathbf{i})(x-1) & 1 \end{pmatrix}, \qquad k = 1, \ldots, q+1, \tag{14}$$

$\gamma_k, \delta_k \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ for $\delta_k^2 \varepsilon - \gamma_k^2 = 1$.

In the same way as in [Lu] we use the strong approximation theorem to prove:

LEMMA 4.12. $\mu(\Lambda(x-1)) \supseteq PSL_2(\mathbb{F}_{q^d})$.

Proof. Since $\mathscr{A}$ splits at x, $G_x^1 \cong SL_2(k_x)$ is not compact and, by Theorem 2.2, $G_k^1 G_x^1$ is dense in $G_{\mathbb{A}}^1$ (see (1) for the notations). Therefore, G_k^1 is dense in $G_{\mathbb{A}}^1 / G_x^1$ and for any open set K of $G_{\mathbb{A}}^1 / G_x^1$, $G_k^1 \cap K$ is dense in K. Hence, for any continuous function $f: K \mapsto \{\text{a finite set}\}$, $f(K) = f(G_k^1 \cap K)$. In particular, this is true for

$$K = G_{1/x}^1 \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij} \in G_{O_{x-1}}^1 \mid a-1, b \equiv 0 \bmod x-1\} \prod_{p \neq x,\, x-1} G_{O_p}^1.$$

Let $\hat{\mu}: K \mapsto SL_2(\mathbb{F}_{q^d}) = SL_2(\mathbb{F}_q[x]/g(x)\,\mathbb{F}_q[x])$ be as follows: For $\xi = (\xi_{1/x}, \ldots, \xi_g = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij}, \ldots)$

$$\hat{\mu}(\xi) = \begin{pmatrix} (a \bmod g) - \mathbf{i}(b \bmod g) & (c \bmod g) - \mathbf{i}(d \bmod g) \\ (x-1)((c \bmod g) + \mathbf{i}(d \bmod g)) & (a \bmod g) + \mathbf{i}(b \bmod g) \end{pmatrix}$$

(i.e., looking only on the g's component, reducing its coefficients modulo g, and then sending it to $SL_2(\mathbb{F}_{q^d})$ by (13)). Since $\xi_g \in G_{O_g}^1$, $\hat{\mu}$ is well defined. Clearly, $\hat{\mu}$ is continuous and $\hat{\mu}(K) = SL_2(\mathbb{F}_{q^d})$, so $\hat{\mu}(G_k^1 \cap K) = SL_2(\mathbb{F}_{q^d})$.

By the definition of K,

$$G_k^1 \cap K = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij} \in H(\mathbb{F}[x, 1/x]) \mid a-1, b \equiv 0 \bmod x-1\}. \tag{15}$$

Considering $\hat{\mu}$ as a function to $PGL_2(\mathbb{F}_{q^d})$, we may multiply every element of $G_k^1 \cap K$ by powers of x. Multiplying by a suitable power of x will force it to be in $\Lambda(x-1)$, so $\hat{\mu}(\Lambda(x-1)) \supseteq PSL_2(\mathbb{F}_{q^d})$. But $\mu = \hat{\mu}$ on $\Lambda(x-1)$; hence $\mu(\Lambda(x-1)) \supseteq PSL_2(\mathbb{F}_{q^d})$. ∎

As the [LPS] Ramanujan graphs, our graphs satisfy a few extremal combinatorial properties.

DEFINITION. Let Γ be a finite connected graph. The *girth* of Γ is the minimal length of a cycle in Γ. The *diameter* of Γ is the maximal distance between any two vertices of Γ. The *chromatic number* of Γ, denoted by $\chi(\Gamma)$, is the minimal number of colors one needs in order to color the vertices of Γ s.t. adjacent vertices have different colors. The *independence number* of Γ, denote by $\iota(\Gamma)$, is the maximal number of vertices of Γ s.t. no two vertices are adjacent.

Recall also the Legendre symbol:

$$\left(\frac{x}{y}\right) = \begin{cases} 1, & x \text{ is a square modulo } y \\ -1, & \text{otherwise.} \end{cases}$$

THEOREM 4.13. *Let q be an odd prime power and ε a nonsquare in $\mathbb{F}_q$. Let $g(x) \in \mathbb{F}_q[x]$ be irreducible of even degree d, and $\mathbb{F}_{q^d}$ is represented as $\mathbb{F}_q[x]/g(x)\,\mathbb{F}_q[x]$. Let $\mathbf{i} \in \mathbb{F}_{q^d}$ $\mathbf{i} \in \mathbb{F}_{q^d}$ be s.t. $\mathbf{i}^2 = \varepsilon$, and*

$$\begin{pmatrix} 1 & \gamma_k - \delta_k \mathbf{i} \\ (\gamma_k + \delta_k \mathbf{i})(x-1) & 1 \end{pmatrix}, \qquad k = 1, \ldots, q+1; \tag{16}$$

$\gamma_k, \delta_k \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ for $\delta_k^2 \varepsilon - \gamma_k^2 = 1$.

a. *If $\left(\frac{x}{g(x)}\right) = 1$. Let Ω_g be the Cayley graph of $PSL_2(\mathbb{F}_{q^d})$ w.r.t. the generators* (16):

1. *Ω_g is a $q+1$ regular Ramanujan graph.*
2. *$|\Omega_g| = (q^{3d} - q^d)/2$, and Ω_g is not bipartite.*
3. $\text{Girth}(\Omega_g) > 2/3 \log_q |\Omega_g| + 1$.
4. $\text{Diameter}(\Omega_g) \leqslant 2 \log_q |\Omega_g| + 2$.
5. *The chromatic number χ of Ω_g satisfies* $\chi(\Omega_g) \geqslant \left((q+1)/2\sqrt{q}\right) + 1$.
6. *The independence number ι of Ω_g satisfies* $\iota(\Omega_g) \leqslant (2\sqrt{q}/(q+1))\,|\Omega_g|$.

b. *If $\left(\frac{x}{g(x)}\right) = -1$. Let Γ_g be the Cayley graph of $PGL_2(\mathbb{F}_{q^d})$ w.r.t. the generators* (16):

1. *Ω_g is a $q+1$ regular Ramanujan graph.*
2. *$|\Omega_g| = q^{3d} - q^d$, and Ω_g is bipartite.*
3. $\text{Girth}(\Omega_g) > 4/3 \log_q |\Omega_g|$.
4. $\text{Diameter}(\Omega_g) \leqslant 2 \log_q |\Omega_g| + 2$.

Proof. a. $\left(\frac{\det(\mu(\xi_k))}{g(x)}\right)=1$, so $\mu(\xi_k)\in PSL_2(\mathbb{F}_{q^d})$. By Lemma 4.12 $\mu(\Gamma_g)=\Omega_g$, and by Theorems 4.10 and 4.11 it is a $(q+1)$-regular Ramanujan graph.

$\Omega_g=PSL_2(\mathbb{F}_{q^d})$ and $|PSL_2(\mathbb{F}_{q^d})|=(q^{3d}-q^d)/2$. Assume that Ω_g is bipartite, i.e., $PSL_2(\mathbb{F}_{q^d})=I\cup O$, and the identity e is in I; then

$$I=\langle \mu(\xi_i)\,\mu(\xi_j) \mid 1\leqslant i,j\leqslant q+1\rangle$$

is a subgroup of $PSL_2(\mathbb{F}_{q^d})$. For any $g\in I$ and any generator $\mu(\xi_k)$

$$\mu(\xi_k)\,g\mu(\xi_k)^{-1}=\mu(\xi_k)\,g\mu(\xi_{(k+(q+1)/2) \bmod (q+1)})\in I.$$

So I is a normal subgroup of $PSL_2(\mathbb{F}_{q^d})$, which is impossible since $PSL_2(\mathbb{F}_{q^d})$ is simple.

In order to bound the girth, it is enough to consider only cycles that begin and end at e. Such a cycle of length t is created by an element $\xi=a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij}=\xi_{i_1}\cdots\xi_{i_t}\in\Lambda(g)$. Clearly,

$$N(\xi)=a^2-b^2\varepsilon+(x-1)(d^2\varepsilon-c^2)=x^t.$$

Since $\mu^2-\eta^2\varepsilon=0$ for $\mu,\eta\in\mathbb{F}_q$ iff $\mu=\eta=0$, t is odd iff $t=\deg(d^2\varepsilon-c^2)+1=\deg(c^2)+1=\deg(d^2)+1$. But g divides c and d, so $t\geqslant 2\deg(g)+1>2/3\log_q|\Omega_g|+1$. If $t=2r$ is even, $N(\xi)\equiv a^2\equiv x^{2r} \bmod g^2$ and g^2 divides $(a-x^r)(a+x^r)$. But $(a,g)=1$; hence, g^2 divides $(a-x^r)$ or g^2 divides $(a+x^r)$. Hence, $r\geqslant 2\deg(g)$ (since $r\geqslant\deg(a)$), and $t\geqslant 4\deg(g)>4/3\log_q|\Omega_g|$.

The proof for the diameter is similar to that in [LPS], using Theorem 4.11 to bound the eigenvalues. A weaker version can be found in [AM].

For the chromatic number see [Ho], and for the independence number a proof due to Alon can be found in [LPS].

b. For any s generators $\mu(\xi_{i_1}),\ldots,\mu(\xi_{i_s})$,

$$\left(\frac{\det(\mu(\xi_{i_1}\cdots\xi_{i_s}))}{g(x)}\right)=\begin{cases}1, & s \text{ is even}\\ -1, & s \text{ is odd.}\end{cases}$$

So $\mu(\xi_{i_1})\cdots\mu(\xi_{i_s})\in PSL_2(\mathbb{F}_{q^d})$ iff s is even, and Ω_g is bipartite. Since $\mu(\Lambda(x-1))\supseteq PSL_2(\mathbb{F}_{q^d})$ and $|PGL_2(\mathbb{F}_{q^d}):PSL_2(\mathbb{F}_{q^d})|=2$, $\mu(\Lambda(x-1))=PGL_2(\mathbb{F}_{q^d})$ and $|PGL_2(\mathbb{F}_{q^d})|=q^{3d}-q^d$.

The bound for the girth is obtained as in part a, using the fact that now t must be even since $N(\xi)\equiv a^2\equiv x^t \bmod g$, and hence $\left(\frac{x^t}{g(x)}\right)=1$. The bound for the diameter is again obtained as in part a. ∎

COROLLARY 4.14. *When* $\deg(g(x))\to\infty$ *we obtain an infinite linear family of* $(q+1)$*-regular Ramanujan graphs.*

5. Explicit Construction for Even q's

Since much is similar to the case of odd q's, we will give the proof only when the difference is fundamental; i.e., when the proof does not appear, it means that it is similar to that of the analogue claim in Section 4 (which is denoted by the same number).

Let q be an even prime power and $f(x)=x^2+x+\varepsilon$ irreducible over $\mathbb{F}_q$. (It is easy to find such $f(x)$, since α is a root of any irreducible z^2+az+b iff α/a is a root of z^2+z+b/a^2.) Let us choose the quaternion algebra:

$$\mathscr{A}=k\mathbf{1}+k\mathbf{i}+k\mathbf{j}+k\mathbf{ij}, \qquad \mathbf{i}^2=\mathbf{i}+\varepsilon,\ \mathbf{j}^2=x,\ \mathbf{ij}=\mathbf{ji}+\mathbf{j}.$$

Here $\bar{\mathbf{i}}=\mathbf{i}+1$, $\bar{\mathbf{j}}=\mathbf{j}$, $\overline{\mathbf{ij}}=\mathbf{ij}$, so for $\xi=a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij}$, $\bar{\xi}=\xi+b$, $\mathrm{tr}(\xi)=b$, and

$$N(\xi)=a^2+b^2\varepsilon+ba+(c^2+d^2\varepsilon+cd)\,x. \tag{17}$$

By Lemma 5.2 $N(\xi)=0$ iff $\xi=0$, so $\mathscr{A}$ is a quaternion algebra. Computing the discriminant of $\mathscr{A}$ we see that the only finite place in which $\mathscr{A}$ is ramified is x, so $1/x$ is also ramified.

Lemma 5.1. *The class number of $\mathscr{A}$ is one.*

Proof. Immediate from [To, Theorem 9]. It is basically the same as the proof of Lemma 4.1. ∎

Then $\mathscr{S}=\mathbb{F}_q[x]\,\mathbf{1}+\mathbb{F}_q[x]\,\mathbf{i}+\mathbb{F}_q[x]\,\mathbf{j}+\mathbb{F}_q[x]\,\mathbf{ij}$ is an integral set in $\mathscr{A}$ ([To, Theorem 6]). Let $N_z=\{\xi\in\mathscr{S}\mid N(\xi)=z\}$.

Lemma 5.2. a. $N_0=\{0\}$, $|N_1|=q+1$.

b. $|N_{x+1}|=(q+1)^2$.

c. *In every coset of $N_1\backslash N_{x+1}$ we can choose a unique representative of the form*

$$\xi=1+\gamma\mathbf{j}+\delta\mathbf{ij}, \qquad \gamma,\delta\in\mathbb{F}_q, \qquad \gamma^2+\gamma\delta+\delta^2\varepsilon=1. \tag{18}$$

which has exactly $q+1$ solutions in $\mathbb{F}_q$.

Proof. For $\alpha,\beta\in\mathbb{F}_q$, $\alpha^2+\alpha\beta+\beta^2\varepsilon=0$ iff $\alpha=\beta=0$ (since if not, $f(\alpha/\beta)=0$). Using this as in the proof of Lemma 4.2, we see that

$$\xi=a+b\mathbf{i}+c\mathbf{j}+d\mathbf{ij}\in N_0\cup N_1\cup N_{x+1}\Rightarrow a,b,c,d\in\mathbb{F}_q.$$

Everything results now from (17), since there are exactly $q+1$ solutions (α,β) in $\mathbb{F}_q$ for $\alpha^2+\alpha\beta+\beta^2\varepsilon=1$. This is true since for $(1,0)\neq(\alpha,\beta)\in\mathbb{F}_q\times\mathbb{F}_q$

$$\alpha^2+\alpha\beta+\beta^2\varepsilon=1 \qquad \text{iff} \quad f(\alpha/\beta)=(\alpha/\beta)^2+(\alpha/\beta)+\varepsilon=1/\beta^2.$$

But any $s \in \mathbb{F}_q$ gives a solution $(\alpha, \beta) = (s/\sqrt{f(s)}, 1/\sqrt{f(s)})$ for $f(\alpha/\beta) = 1/\beta^2$ (since $f(s) \neq 0$). This, of course, leads to q different solutions, and $(1, 0)$ is one more. ∎

DEFINITION 5.3. $\xi_1, \ldots, \xi_{q+1}$ of (18) are called the *basic norm* $x+1$. Here $\overline{\xi_i} = \xi_i$.

LEMMA 5.4. *A quaternion $t \in \mathcal{S}$, with $N(t) = (x+1)^n$ for some integer n, has the unique factorization*

$$t = (x+1)^r u \theta_1 \cdots \theta_m, \tag{19}$$

where $2r + m = n$, $N(u) = 1$, θ_i are basic norm $x+1$, and $x+1$ does not divide $\theta_1 \cdots \theta_m$.

THEOREM 5.5. *A quaternion $t = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \mathcal{S}$ with $N(t) = (x+1)^n$ for some integer n is a multiple of basic norm $x+1$ iff*

$$a - 1, b \equiv 0 \bmod x. \tag{20}$$

DEFINITION 5.6.

$$\Lambda(x) = \left\{ t = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \mathcal{S} \;\middle|\; \begin{array}{l} a - 1, b \equiv 0 \bmod x, \\ N(t) \text{ is a power of } x+1, \\ x+1 \text{ does not divide } t. \end{array} \right\}$$

COROLLARY 5.7. *$\Lambda(x)$ is a free product of $q+1$ groups of order 2:*

$$\Lambda(x) = \langle \xi_1 \rangle \langle \xi_2 \rangle \cdots \langle \xi_{q+1} \rangle.$$

$\mathcal{A}$ splits at $x+1$, so we have

$$\theta: \mathcal{A}_{x+1} \cong M_2(k_{x+1})$$

and $\theta: \Lambda(x) \subsetneq PGL_2(k_{x+1}) = G'_{x+1}$. $\Lambda(x)$ or more precisely $\theta(\Lambda(x))$ acts on the three $T_{x+1} = G'_{x+1}/G'_{O_{x+1}}$.

LEMMA 5.8. *The action of $\Lambda(x)$ on T_{x+1} is simply transitive. So T_{x+1} can be identified with the Cayley graph of $\Lambda(x)$ w.r.t the basic norm $x+1$ as generators.*

Proof. As in the proof of Lemma 4.8, $\xi_i G'_{O_{x+1}}$ is a neighbor of the root $1G'_{O_{x+1}}$ of T_{x+1}. Again a stabilizer is compact and discrete and, hence, of finite order. But for $i \neq j$ $\xi_i \xi_j$ is not of finite order, so

$\xi_1 G'_{O_{x+1}}, \ldots, \xi_{q+1} G'_{O_{x+1}}$ are exactly all the $q+1$ neighbors of $1G'_{O_{x+1}}$. Since $G'_{O_{x+1}}$ acts as a group of automorphisems of T_{x+1}, we know that $g\xi_1 G'_{O_{x+1}}, \ldots, g\xi_{q+1} G'_{O_{x+1}}$ are all the $q+1$ neighbors of $gG'_{O_{x+1}}$. This shows that the action is transitive and that no stabilizer (different from one) is possible. ∎

Let $g(x) \in \mathbb{F}_q[x]$ be any polynomial which is prime to $x(x+1)$, and $d = \text{degree}(g(x))$.

DEFINITION 5.9. $\Lambda(g) = \{\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij} \in \Lambda(x) \mid b, c, d \equiv 0 \bmod g(x), (a, g) = 1\}$. $\Gamma_g = \Lambda(g)\backslash T_{x+1}$ $(= \Lambda(g)\backslash G'_{x+1}/G'_{O_{x+1}} = \Lambda(g)\backslash\Lambda(x))$.

THEOREM 5.10. *Γ_g is a finite $g+1$ regular graph. Moreover, Γ_g is the Cayley graph of the group $\Lambda(g)\backslash\Lambda(x)$ w.r.t. the $q+1$ basic norm $x+1$ as generators.*

THEOREM 5.11. *Let μ be any eigenvalue of the adjacency matrix of Γ_g; if $\mu \neq \pm(q+1)$ then $|\mu| \leqslant 2\sqrt{q}$. In particular, Γ_g is a Ramanujan graph.*

For the sake of simplicity, assume that $g(x)$ is irreducible of even degree. Therefore there is an $\mathbf{i} \in \mathbb{F}_{q^d} \cong \mathbb{F}_q[x]/g(x)\,\mathbb{F}_q[x]$ s.t. $f(\mathbf{i}) = \mathbf{i}^2 + \mathbf{i} + \varepsilon = 0$ and define $\mu: \Lambda(x) \to PGL_2(\mathbb{F}_{q^d}) = PSL_2(\mathbb{F}_{q^d})$ by

$$\mu(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{ij}) = \begin{pmatrix} a + b\mathbf{i} & c + d\mathbf{i} \\ x(c + d\mathbf{i} + d) & a + b\mathbf{i} + b \end{pmatrix}.$$

Clearly $N(\xi) = \det(\mu(\xi))$. The kernel of μ is $\Lambda(g)$, so Γ_g is the Cayley graph of $\mu(\Lambda(x))$ with respect to the $q+1$ generators:

$$\mu(\xi_k) = \begin{pmatrix} 1 & \gamma_k + \delta_k\mathbf{i} \\ (\gamma_k + \delta_k\mathbf{i} + \delta_k)\,x & 1 \end{pmatrix}, \qquad k = 1, \ldots, q+1. \tag{21}$$

$\gamma_k, \delta_k \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ for $\gamma_k^2 + \gamma_k\delta_k + \delta_k^2\varepsilon = 1$.

LEMMA 5.12. $\mu(\Lambda(x)) = PSL_2(\mathbb{F}_{q^d}) = PGL_2(\mathbb{F}_{q^d})$.

THEOREM 5.13. *Let q be a power of 2 and $f(x) = x^2 + x + \varepsilon$ irreducible in $\mathbb{F}_q[x]$. Let $g(x) \in \mathbb{F}_q[x]$ be irreducible of even degree d, and $\mathbb{F}_{q^d}$ is represented as $\mathbb{F}_q[x]/g(x)\,\mathbb{F}_q[x]$. Let $i \in \mathbb{F}_{q^d}$ be a root of $f(x)$, and*

$$\begin{pmatrix} 1 & \gamma_k + \delta_k i \\ (\gamma_k + \delta_k i + \delta_k)\,x & 1 \end{pmatrix}, \qquad k = 1, \ldots, q+1; \tag{22}$$

$\gamma_k, \delta_k \in \mathbb{F}_q$ are all the $q+1$ solutions in $\mathbb{F}_q$ for $\gamma_k^2 + \gamma_k \delta_k + \delta_k^2 \varepsilon = 1$. Let Γ_g be the Cayley graph of $PSL_2(\mathbb{F}_{q^d})$ w.r.t. the generators (22). *Then:*

1. *Γ_g is a $(q+1)$-regular Ramanujan graph.*
2. *$|\Gamma_g| = q^{3d} - q^d$, and Γ_g is not bipartite.*
3. $\text{Girth}(\Gamma_g) \geqslant 2/3 \log_q |\Gamma_g|$.
4. $\text{Diameter}(\Gamma_g) \leqslant 2 \log_q |\Gamma_g| + 2$.
5. *The chromatic number χ of Γ_g satisfies $\chi(\Gamma_g) \geqslant ((q+1)/2\sqrt{q}) + 1$.*
6. *The independence number ι of Γ_g satisfies $\iota(\Gamma_g) \leqslant (2\sqrt{q}/(q+1))|\Gamma_g|$.*

COROLLARY 5.14. *When* $\text{degree}(g(x)) \to \infty$ *we obtain an infinite linear family of $(q+1)$-regular Ramanujan graphs.*

ACKNOWLEDGMENTS

I thank my advisors A. Lubotzky and E. Shamir for fruitful discussions and encouragement. N. Pippenger is gratefully acknowledged for valuable comments.

REFERENCES

[Al] N. ALON, Eigenvalues and expanders, *Combinatorica* **6**, No. 2 (1986), 83–96.

[Alb] A. A. ALBERT, "Structure of Algebras," Amer. Math. Soc., New York, 1939; revised, 1961.

[AM] N. ALON AND V. MILMAN, λ_1, isoperimetric inequalities for graphs, and superconcentrations, *J. Combin. Theory Ser. B* **38** (1985), 73–88.

[Co] E. COHEN, Sums of an even number of squares in $GF[p^n, x]$, II, *Duke Math. J.* **14** (1947), 543–557.

[Di] L. E. DICKSON, "Algebras and Their Arithmetics," Univ. of Chicago Press, Chicago, 1923.

[Dr] V. G. DRINFELD, The proof of Peterson's conjecture for $GL(2)$ over global field of characteristic p, *Functional Anal. Appl.* **22** (1988), 28–43.

[Ge] S. GELBART, "Automorphic Forms on Adele Groups," Princeton Univ. Press, Princeton, NJ, 1975.

[GG] O. GABER AND Z. GALIL, Explicit construction of linear sized superconcentrators, *J. Comput. System Sci.* **22** (1981), 407–420.

[GGPS] I. M. GELFAND, M. I. GRAEV, AND I. I. PYATETSKII-SHAPIRO, "Representation Theory and Automorphic Functions," Saunders, Philadelphia, 1969.

[Ho] A. J. HOFFMAN, On eigenvalues and coloring of graphs, *in* "Graph Theory and its Applications" (B. Harris, Ed.), pp. 79–91, Academic Press, New York, 1970.

[Kl] M. KLAWE, Limitations on explicit constructions of expanding graphs, *SIAM J. Comput.* **13** (1984), 155–156.

[La] S. LANG, "$SL_2(R)$," Springer-Verlag, New-York, 1985.

[LPS] A. LUBOTZKY, R. PHILLIPS, AND P. SARNAK, Ramanujan graphs, *Combinatorica* **8**, No. 3 (1988), 261–277.

[Lu] A. LUBOTZKY, Discrete groups, expanding graphs and invariant measures, *Birkhauser Progress in Math.*, to appear.

[Ma] G. A. MARGULIS, Explicit construction of concentrators, *Problems Inform. Transmission* **11** (1975), 325–332.

[Ma1] G. A. MARGULIS, Explicit group theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators, *Problems Inform. Transmission* **24** (1988), 39–46.

[Mo] M. MORGENSTERN, "Ramanujan Diagrams and Explicit Construction of Expanding Graphs," Ph.D. thesis, Hebrew University of Jerusalem, 1990.

[Pin] M. S. PINSKER, On the complexity of a concentrator, *in* "Proceedings, 7th International Teletraffic Conf. Stockholm, 1973."

[Pip] N. PIPPENGER, Superconcentrators, *SIAM J. Comput.* **6** (1972), 298–304.

[Pr] G. PRASAD, Strong approximation for semi-simple groups over function fields, *Ann. of Math.* **105** (1977).

[Re] I. REINER, "Maximal Orders," Academic Press, New York, 1975.

[Se] J. P. SERRE, "Trees," Springer-Verlag, New York/Berlin, 1980.

[Sh] V. SHOUP, New algorithms for finding irreducible polynomials over finite fields, *in* "29th Annual Symposium on Foundations of Computer Science, 1988," pp. 283–290.

[To] L. TORNHEIM, Integral sets of quaternion algebras over function fields, *Trans. Amer. Math. Soc.* **48** (1940), 436–450.

[Vi] M. F. VIGNERAS, "Arithmétique des Algèbres de Quaternions," Lecture Notes in Math., Vol. 800, Springer-Verlag, New York/Berlin, 1980.

[We] A. WEIL, "Basic Number Theory," Springer-Verlag, New York/Berlin, 1967.